PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Commissioner
US Department of Commerce
United States Patent and Trademark Office, PCT
2011 South Clark Place Room CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 06 June 2001 (06.06.01)	
International application No. PCT/US00/17395	**Applicant's or agent's file reference** RCA89673
International filing date (day/month/year) 23 June 2000 (23.06.00)	**Priority date** (day/month/year) 15 July 1999 (15.07.99)
Applicant KNOKE, Kevin, Charles et al	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

09 February 2001 (09.02.01)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Henrik Nyberg
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

PORT COVER FOR LIMITING TRANSFER OF ELECTROMAGNETIC RADIATION FROM A PORT DEFINED IN A HOST DEVICE

BACKGROUND OF THE DISCLOSURE

1. Field of the Invention

The invention relates to host devices. More particularly, the invention relates to a port cover for a host device.

2. Description of the Prior Art

Smart cards, and other similar information-storing devices, are known for their capabilities in storing information relating to stored funds, personal identification and other personal data, descrambling keys and an ability to access certain host devices.When multiple users share a common host device, each user may have a separate smart card having selected limitations, these limitations are triggered, e.g., when one user's smart card is removed from a host device and another user's smart card is inserted into the host device.

It is difficult to provide an interface between smart cards and certain host devices that emit certain ranges of electromagnetic radiation. For example, satellite receivers formed as set top boxes are configured as enclosed boxes with an electromagnetic/radio frequency interference shield (EMI/RFI shield) entirely covering each wall of the satellite receiver. If a satellite receiver is provided with a smart card port to provide access to the smart card, the smart card port would provide an opening in which little or no EMI/RFI shield would exist. With a lack of an EMI shield over even a portion of the host device, electromagnetic interference (EMI), possibly including radio frequency interference (RFI), could escape from the satellite receiver into the surrounding space. This large emission of EMI is unacceptable, since it does not conform with industry standards and can result in interference applied to electronic equipment located in the vicinity.

It would be desirable to provide a configuration for a host device having a smart card port in which the entire satellite receiver can be shielded to limit emissions of EMI generated by the host device into the surrounding areas.

Hackers present another concern by attempting to "use" information obtained from other smart cards. One technique that accomplishes this unauthorized accessing of information is referred to as hot-wiring a smart card. This hot-wiring is accomplished by affixing a single wire to each smart card contact. The smart card is then inserted into the host device and the host device begins to interact with the smart card with the hot-wiring wire extending out of the port. During this interaction, confidential information may be electronically

transferred between the host device and the smart card, and thereby is also transmitted outside of the host device through the hot-wiring wires, via the port. If a hacker uses suitable equipment outside the host device, the hacker can obtain much of the confidential information that is on the smart card, and can also produce a copy of the smart card that might be used in place of the original.

Therefore, a need exists in the art for a device to limits hot-wiring of the smart card. This device will improve security associated therewith by preventing unauthorized use of access codes and breach of confidentiality, thereby improving user confidence in, and acceptance of, the system.

SUMMARY OF THE INVENTION

The present invention relates to a port cover for covering the port formed in a host device, the port cover includes a bottom portion, a plurality of side portions, and couplers to attach the sides to a host device, where said couplers attach on either side of the port.

BRIEF DESCRIPTION OF THE DRAWINGS

The teachings of the present invention can be readily understood by considering the following detailed description in conjunction with the accompanying drawings, in which:

FIG. 1 shows a schematic diagram of a satellite/TV receiver system in accordance with one embodiment of the present invention;

FIG. 2 shows a cross sectional expanded view of a smart card inserted into a host device in accordance with one embodiment of the present invention;

FIG. 3 shows a partial cross-sectional view of one embodiment of a port cover in accordance with the present invention;

FIG. 4 shows a perspective view of one embodiment of the port cover of FIG. 3;

FIG. 5 shows a perspective view of an alternate embodiment of the port cover 302 of Fig. 3.

To facilitate understanding, identical reference numerals have been used, where possible, to designate identical elements that are common to the figures.

DETAILED DESCRIPTION

After considering the following description, those skilled in the art will clearly realize that the teachings of the invention can be readily utilized in satellite/TV receiver systems, or any other host device that uses a smart card or other similar information-storing device.

FIG. 1 shows a typical satellite/TV receiver system 100 that includes a satellite receiver 101, a satellite dish 102, and a television 104. The integration and operation of system 100 (particularly controller 107, CPU 114, memory 116, I/O 118 and bus 119) is well known and thus is not described herein

Satellite receiver 101 includes smart card portion 106 and controller portion 107. Smart card portion 106 includes the removable smart card 108, a smart card port 112, a smart card collar 113, and a smart card reader 110. The smart card reader 110 includes smart card reader head 111. In one embodiment, the smart card 108 includes a smart card operating patch 109. The smart card port 112 permits insertion of, and removal of, different selected smart cards through the smart card port 112. Smart card collar 113 retains the smart card 108 in position when a smart card 108 is inserted through the smart card port 112. The smart card port 112 is formed in a housing 121 that defines the outer surface of the satellite receiver 101.

Smart card 108 is further detailed in cross section in FIG. 2. Smart card operating patch 109, formed on an external surface of smart card 108, includes smart card contacts 202a, 202b, 202c, and 202d, integrated circuit 205, and insulative material 204 (e.g., resin) that secures contacts 202 in position. Each smart card contact is electrically connected by conductors to integrated circuit 205. The surface of each smart card contact is exposed to an external surface 201 of smart card 108 at smart card operating patch 109 such that an electric probe touching the exposed surface at each smart card contact can transmit signals to, and receive signals from, the integrated circuit 205. The primary function of integrated circuit 205 (which may be an application specific integrated circuit) is to store information (some of which may be modified). The information that is to be saved may include monetary amounts, programming capabilities, individual and address information, and other such information, such as descrambling keys.

The smart card reader 110 is also depicted in FIG. 2 in a position that it would be when interacting with the smart card contacts. The smart card reader 110 includes a plurality of smart card contacts 206a, 206b, 206c, and 206d which electrically connect to smart card contacts 202a, 202b, 202c, and 202d, respectively, when the smart card is inserted in the smart card port 112. Although four smart card contacts 206a-d are depicted in FIG. 2, any suitable number of smart card contacts can be selected for the intended task, such as, e.g., eight depicted in FIG. 3.

During use, different smart cards may be removed from, and inserted into, satellite receiver 101. In a household, for example, different members may have different television channels that their smart cards can access, or certain users may by allowed only a certain amount of use of the satellite receiver 101 (and the associated television 104) each week. Any card, chip, or other device that provides similar interactive capabilities with a host device as described herein is intended to be within the scope of the smart card of the present invention. Any host device capable of interacting with a smart card, such as a television set-top cable or satellite box, flash memory modules used in digital cameras, so-called MP players, etc. are within the intended scope of the present invention.

Two problems exist relative to the above-mentioned smart card 108 and host device 101 configuration that a port cover 302, shown in FIG. 3 and described below, is intended to overcome. A first electromagnetic interference (EMI)/ radio frequency interference (RFI) shielding problem results from the EMI or RFI produced by the satellite receiver 101. Typically, the housing 121 of satellite receivers 101 are formed to shield electromagnetic radiation. The smart card port 112 however defines a breach in the EMI/RFI shielding by which the EMI/RFI can escape form the host device or satellite receiver 101. Such a breach in the EMI/RFI shielding in the satellite receiver severely limits the approval of the satellite receiver 101 by appropriate governmental communication radiation regulatory agencies.

A second, security related, problem with smart cards results when any unauthorized smart card user attempts to access either the host device or information contained in the smart card. The fact that the smart card operating patch 109 is physically located within the satellite receiver 101 as shown in FIG. 1 is a first effort to limit unauthorized users from gaining access to the information contained within the smart card, when the smart card 108 is positioned within the satellite receiver 101 by limiting unauthorized users access to the smart card contacts 206a-d. One technique by which unauthorized users gain access to information contained within the smart card 108 is to electrically connect a distinct, appropriately sized, electrically conductive wire (referred to herein as hot-wired wire 212 depicted in FIG. 2) to each distinct smart card contact 202a, 202b, 202c, and 202d. Thus, when the smart card 108 is inserted into the smart card port causing each smart card contact 202 to contact the respective reader head contact 206, then any signal transmitted between the smart card reader head 111 and the smart card 108 could be read at the other end of the hot-wired wire 212, which would extend out of the smart card port

112. This unauthorized accessing of information contained in the smart card is referred to herein as "hot-wiring" the smart card.

Port Cover

Port cover 302 is mounted over smart card port 112 after the smart card is inserted into the smart card port. The use of the port cover 302 has two primary functions. First, the port cover 302 limits EMI (including RFI) that can escape from the EMI/RFI shield after the port cover is in place. Second, the port cover 302 limits the use of the host device (e.g. satellite receiver 101) if the smart card 108 is being hot-wired. With the port cover 302 in place, the remote end of the hot-wired wires 212 cannot physically extend from within the satellite receiver 101, through the smart card port cover 302, to outside of the satellite receiver. The port cover 302 is preferably configured as a snap-on, electroless metal plated plastic cover. The port cover 302 is configured to cover the port while a National Renewable Security Standard (NRSS) smart card 108, or the like, is installed therein.

Port cover 302 includes body portion 303, peripheral mounting surface 304 coupling pads 306a and 306b, mounting flanges 308, and small spherical bumps 416. Body portion 303 forms the cover to limit access into the smart card port 112. Body portion 303, depicted in FIG. 3, includes bottom portion 330, and multiple side portions 330, 334, 336 that extend from the peripheral mounting surface 304 to the bottom portion 330. The bottom portion 330, side portions 330, 334, and 336, and peripheral mounting surface (when the port cover 302 is installed) define an enclosure that combines with the satellite receiver 101 to delineate an interior space where the satellite receiver 101 components are located from an outside space 322. Radiation contained within the interior space is shielded from passing into the outside space 322. A peripherally extending surface 309 is formed in the housing 121 and extends around the periphery of the smart card port 112. A peripheral mounting surface 304 mounts with the peripherally extending surface 309 in a manner that no wires can extend between the two surfaces when the port cover 302 is installed.

Coupling pads 306a, 306b have two functions. First, each distinct coupling pads 306a, 306b enter into a distinct mating recesses 310 to securely position the port cover 302 over smart card port 112. Second, coupling pad 306a contacts electrical source contact (not depicted but contained in first mating recess 310 that coupling pad 306a engages with) while coupling pad 306b contacts electrical drain contact (not depicted but contained in second mating recess 310 that coupling pad 306b engages with) causing an electrical

voltage to be applied as described below. Mounting flanges 308 also extend into recesses 314 to assist in securing the port cover 302 to the peripherally extending surfaces 309. Port cover 302 is preferably formed form a resilient plastic that permits the coupling pads 306a, 306b, and the mounting flanges 308 to be displaced relative to each other as a result of a moderate biasing force. This relative displacement permits the coupling pads to be inserted into the mating recesses 310, and the mounting flanges 308 to be inserted into the recesses 314 to a position where tangs 340 snap back into position and secure the port cover in position covering the entire port cover. When the tangs 340 are securing the port cover in position, release portions 342 may be pressed to deflect the tangs, and release the coupling pads 308 from the mating recesses 310 while the mounting flanges 308 are removed from recesses 314. Small spherical bumps 416 extend from the peripheral mounting surface 304 to ensure grounding of the peripheral mounting surfaces 304 to the peripherally extending surface 309, thereby grounding port cover 302 to housing 121.

Formed in housing 121 of satellite receiver 101 is EMI/RFI shield 320. However, the EMI/RFI shield 320 does not extend over smart card port 112 which defines a breach in the EMI/RFI shield. To limit escape of EMI/RFI that passes through smart card port 112 into the surrounding environment (depicted as 322 in FIG. 3), port cover 302 is provided with EMI/RFI cover shielding 322, which is selected to be a suitable material to shield the EMI or RFI that is likely to be produced within the satellite receiver 101. As the port cover is positioned such that: a) coupling pads 306a, 306b are positioned within mating recesses 310, b) mounting flanges 308 are positioned into recesses 314, and c) peripheral mounting surface 304 abuts peripherally extending surface 309; then EMI/RFI enclosure 324 is formed within EMI/RFI cover shield 322 that limits passage of EMI and/or RFI from within the EMI/RFI cover shield to the surrounding environment 322.

The use of hot-wired wires by hackers to tamper with or access information contained on smart card 108 has been described above. There are two embodiments of port covers 302 depicted in FIGs. 3, 4, and 5 that limit the use of hot-wired wires 212. In considering the two embodiments of port covers 302, FIG. 3 should be viewed in combination with FIG. 4 for the first embodiment. FIG. 3 should be viewed in combination with FIG. 5 when considering the second embodiment.

There are two distinct embodiments of the present invention depicted in FIGs. 4 and 5, respectively. Both embodiments of the present invention limits access of information across the hot-wired wire to a remote end of the hot-wired

wire from the contact 202a, via the smart card port 112 to a location outside the port cover 302. Since the entire length of the hot-wired wire 112 would be either positioned within either the host device; e.g., the satellite receiver 101, or the port cover 302, a hacker is restricted from accessing a hot-wired wire 212 when the port cover 302 is in place.

The first embodiment of the present invention (depicted in FIG. 4) involves the use of a conductor trace 412. Conductor trace 412 functions to limit an unauthorized user from drilling through the port cover 302 such that hot-wired wires 212 can be passed through the holes in port cover 302. The conductor trace covers top portion 330, front portion 332, bottom portion 334, and the two side portions 336. The conductor trace 412 is to be configured such that if a hacker drills through the port cover 302 at any location that might provide access for the hot-wired wires 212, then at least one individual conductor 414 in conductor trace 412 will be severed. The individual conductors 414 of the conductor trace 412 are preferably arranged in parallel. Therefore, severing of any of the individual conductor(s) 414 will alter the electrical characteristics (e.g., the impedance) of the entire conductor trace 412. Therefore, the conductor trace can be monitored for changes in impedance, indicating tampering of port cover 302. Additionally, if port cover 302 is not positioned over smart card port 112, then the coupling pads 306a and 306b will not engage with mating recess 310 and electric current will not pass between the two mating recesses 310 associated with two coupling pads 306a and 306b.

It is preferable for the conductors to form conductor trace 412 to cover as much of the surface area of port cover 302 as possible, with as little spacing between the individual conductors 414 of the conductor trace as possible. This will limit the possibility that a hacker will be able to drill between the individual conductors 414 forming the conductor trace 412 in that the hacker may attempt to cut or drill around the individual conductors, if they can see where they are located.

There are a variety of techniques by which conductor trace 412 is formed. In a first conductor trace formation technique, the conductors are applied to the port cover via selective plating or conductive powder coating. In selective plating, a conductive material is plated onto the surface of the port cover 302. A conductive material that can adhere to the material that the port cover is formed from (preferably plastic), is required. In conductive powder coating, an adhesive (not shown) following the outline of the individual conductors is placed on the desired surfaces of the port cover 302, and a powder formed from a conductive material is applied to the adhesive. The conductive powder "sticks" to the

adhesive, thereby forming the conductors in the conductor trace 412. In an alternate embodiment, the individual conductors 414 of the conductor trace 412 are affixed to the port cover 302 by a resin such as epoxy. The surface above the individual conductors of the conductor trace 412 should be painted so hackers cannot determine the precise positioning of the individual conductors 414 in the conductor trace 412. The technologies used to form the conductor trace are generally known, and will not be further detailed herein. Any known technique by which a conductor trace 412 is applied to port cover 302 is within the scope of the present invention.

Even though the term "electric current" is used in this specification and the associated claims, it is intended that related electrical measurements such as electric voltage, electrical voltage or current of a prescribed frequency or waveform, etc., are within the scope of the present invention. It is also envisioned that magnetic characteristics can be measured across the conductor trace 412 using known detector systems that can interface with controller 107. The conductor trace 412 may be configured as either an active or passive circuit. However, any technique that securely attaches, or forms, the individual conductors 414 to the port cover 302 is within the intended scope of the present invention.

In the second embodiment of applying conductor trace 412 to port cover 302 (depicted in FIG. 5 as taken relative to FIG. 3), the conductor trace 412 in the FIG. 4 embodiment is replaced by conductive plating 500 (shown by shading) applied to the port cover 302. More specifically, the conductive plating extends over top portion 330, front portion 332, bottom portion 334, and the two side portions 336. The conductive plating 500 is connected by insulated conductors 504a, 504b to coupling pads 306a, 306b, respectively. Alternatively, the above-described conductive plating and conductive powder technologies, described relative to the FIG. 4 embodiment, may be applied in this embodiment as well to form a substantially continuous conductor over the port cover 302. Insulated conductors 504a and 504b are depicted as attached to the surface of peripheral mounting surface 304 in FIG. 5, however the insulated conductors may actually be integrated in port cover 302. Conductive plating has empirically determinable electrical resistivity characteristics that are altered by tampering, such as cutting through, or drilling in, the body portion 303. Inner or outer surfaces of conductive plating 500 may contain an insulative coating (not shown) to limit grounding of the conductive plating 500 to the port cover 302. This insulative coating is not necessary if the port cover 302 is formed from an insulative plastic. As a result of such cutting or drilling in the body portion 303,

which will necessarily cause similar cutting or drilling of the conductive plating 500 that plates the body portion 303, the electrical characteristics of the conductive plating 500 will be altered. This altering of the electrical characteristics of the conductive plating 500 can be sensed as a varying impedance, resistance, or other measurement in a similar manner that the electrical characteristics of the electrical trace 412 was altered in the FIG. 4 embodiment when individual conductors were severed.

The FIGs. 3 and 4 port cover embodiment, as well as the FIGs. 3 and 5 port cover embodiment, may be controlled by controller 107 as depicted in FIG. 1. Considering the above disclosure, controller 107 may encounter three possible alternative conditions relating to the electric level of the electric contacts formed in mating recess 310 (not shown):

a) when no electric current is sensed between the electric contacts formed in the two mating recesses 310, controller 107 determines that there is no port cover 302 in place. Under these conditions, controller 107 will not interact with the smart card 108;

b) when a predetermined limit of electric current is sensed between the electric contacts formed in the two mating recesses 310, controller 107 determines that the port cover is in place, and none of the individual conductors 414 in the conductor trace 412 have been tampered with. Under these circumstances, controller 107 will interact with the smart card 108; or

c) when some range of electric current between the "no electric current" sensed in part a) and the "predetermined limit" of part b) is sensed between the electric contacts formed in the two mating recesses 310, controller 107 determines that at least one of the individual conductors 414 in the conductor trace 412 have been tampered with (e.g., a conductor has been damaged, presumably by drilling or cutting through the port cover 302). Under these circumstances, controller 107 will not interact with the smart card 108.

The level of the predetermined limit is based on the specific circuit, and is preferably determined empirically.

Though various embodiments which incorporate the teachings of the present invention have been shown and described in detail herein, those skilled in the art can readily devise many other varied embodiments that still incorporate these teachings.

What is claimed is:

1. A method of securing information being transferred from an information-storing device interacting with a host device through a port formed in the host device, the port being configured to receive the information-storing device, the method comprises the acts of:

positioning a port cover over the port;

supplying an electric signal to a conductor formed in the port cover; and

monitoring the electric signal to ensure that the port cover is correctly positioned and the conductor is not breached.

2. The method set forth in claim 1, further comprising the act of limiting interaction by a host device with the information-storing device if the monitored electric signal exceeds a predetermined parameter.

3. The method set forth in claim 1, wherein the host device is a satellite receiver.

4. A port cover for covering a port formed in a host device, the port cover comprising:

a bottom portion;

a plurality of side portions; and

couplers to attach the sides to a host device, where said couplers attach on either side of the port.

5. The port cover set forth in claim 4, further comprising conductive plating extending over the bottom portion and the plurality of side portions.

6. The port cover set forth in claim 4, further comprising a conductive trace extending over the bottom portion and the plurality of side portions.

7. An apparatus for use with a smart card, the apparatus comprising:

a host device capable of accessing information stored in the smart card, the host device including a housing having a port formed therein, the port is configured to receive the smart card, when the smart card is inserted into the port, information can be transferred from the smart card to the host device; and

a port cover removably coupled to the housing surrounding the port, the port cover entirely covers the port.

8. The apparatus set forth in claim 7, wherein the housing and the port cover comprises shielding for electromagnetic interference.

9. The apparatus set forth in claim 8, wherein the shielding comprises a conductive plating.

10. The apparatus set forth in claim 7, wherein a data stream can be transferred between the smart card and the host device, when the smart card is inserted in the port and the port cover is covering the port.

11. The apparatus set forth in claim 7, wherein when the port cover is installed, electrical wires electrically connected to the smart card are limited from extending through the port from within the host device to outside of both the host device and the port cover.

12. The apparatus set forth in claim 7, wherein the housing includes a mounting flange extending peripherally of the port, wherein when the port cover is attached to the mounted flange, the port cover covers the entire port such that the housing and the port cover define an enclosure.

13. The apparatus set forth in claim 7, further comprising:

at least one conductor attached to the port cover;

an electric sensor sensing a breach of the conductor; and

a limiting device limiting operation of the host device when the conductor is breached.

14. The apparatus set forth in claim 13, wherein the electric sensor senses an electric current that deviates from the predetermined range to indicate that the conductor is breached.

15. The apparatus set forth in claim 13, wherein the conductor comprises a plurality of wires arranged in parallel extending across the port cover.

16. The apparatus set forth in claim 13, wherein the conductor comprises a conductive plate.

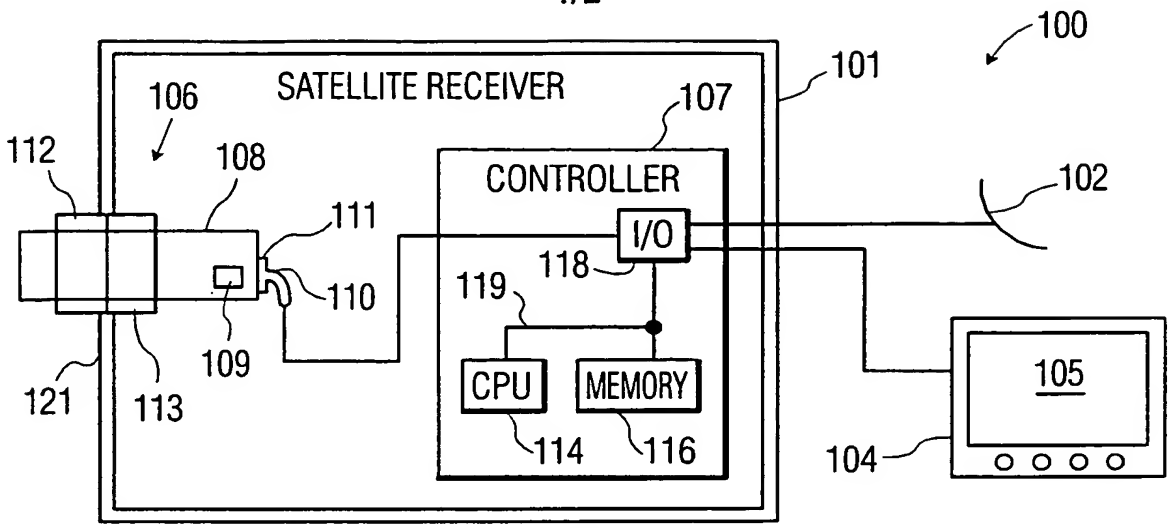

FIG. 1

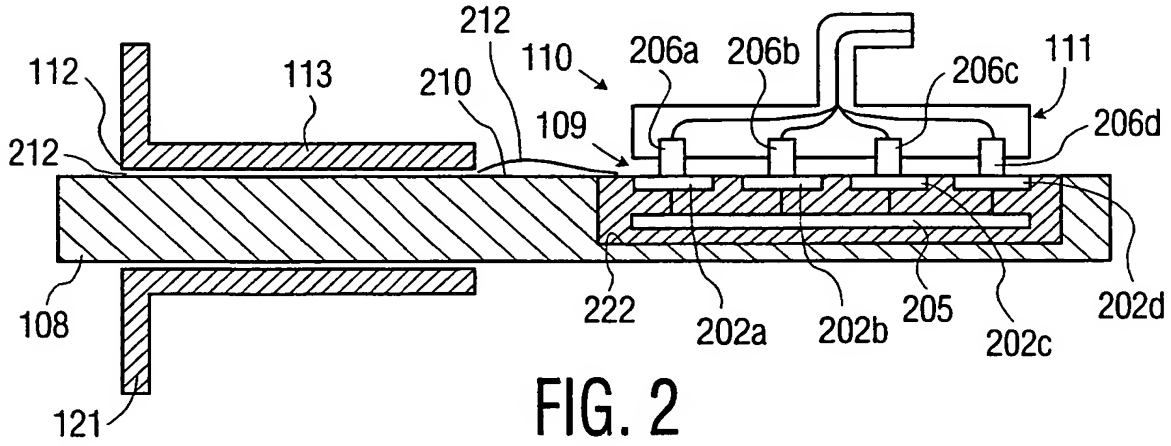

FIG. 2

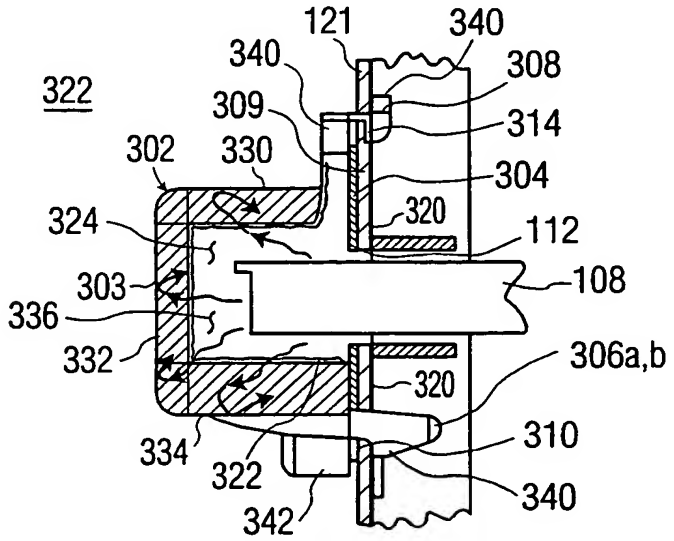

FIG. 3

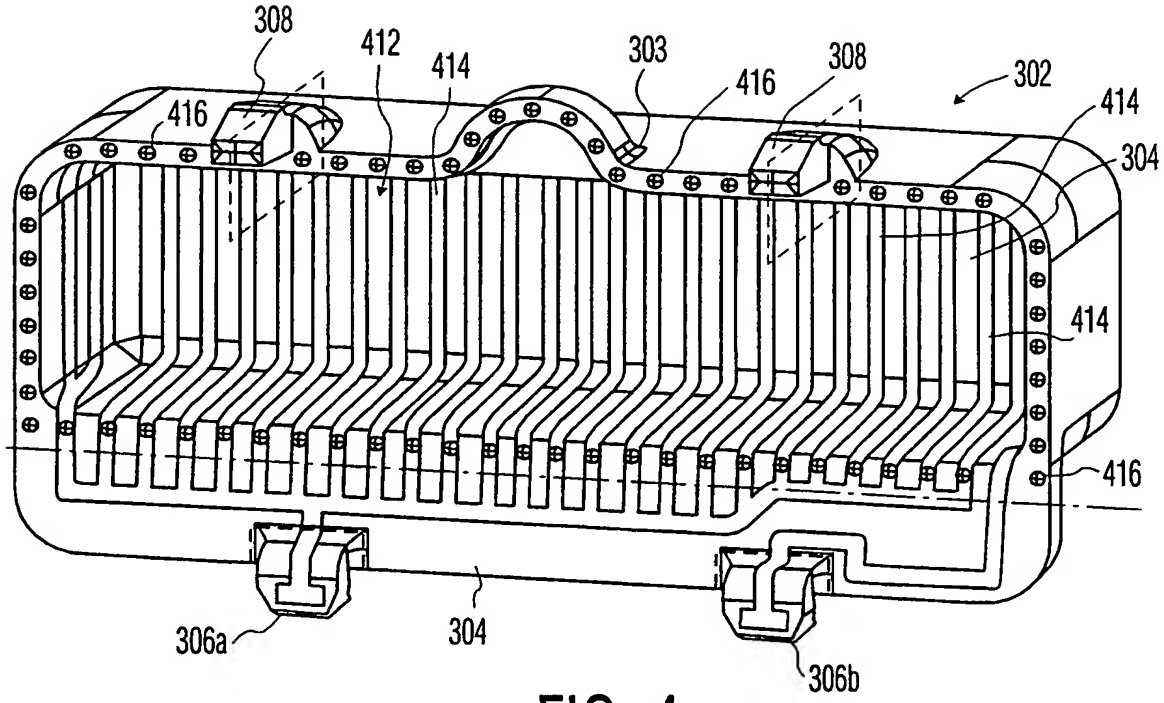
308
412
414
303
416
308
302
414
304
416
414
416
306a
304
306b

FIG. 4

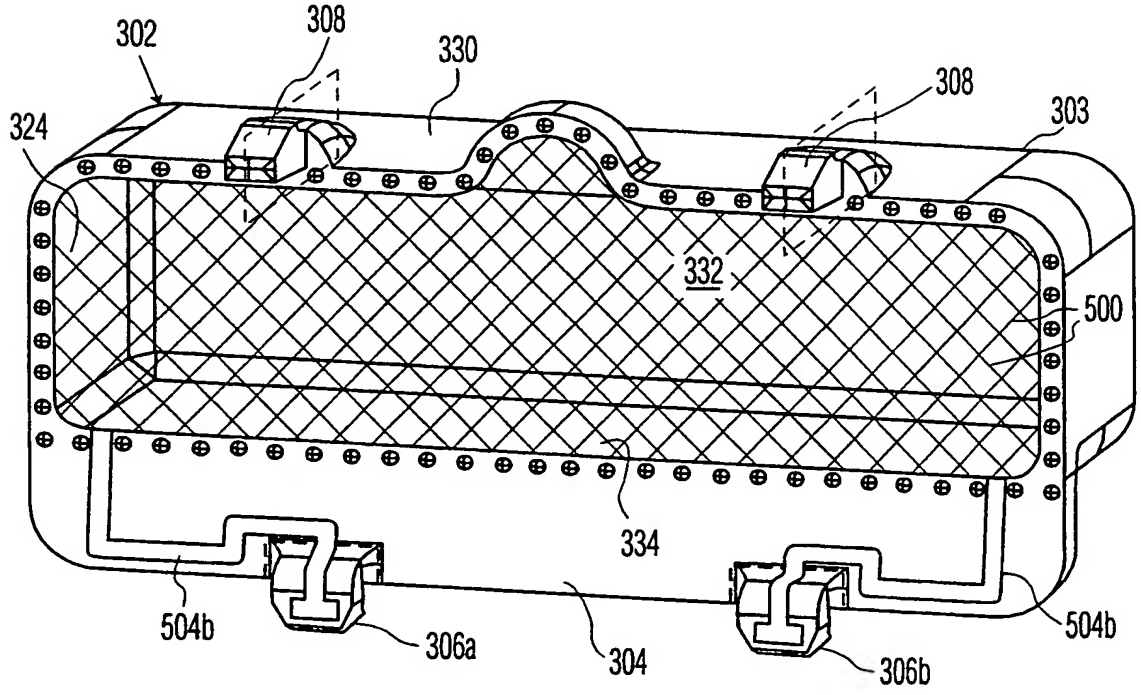
302
308
330
324
308
303
332
500
334
504b
306a
304
306b
504b

FIG. 5

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION** see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
RCA89673		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US 00/ 17395	23/06/2000	15/07/1999
Applicant		
THOMSON LICENSING S.A.		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

   a. With regard to the **language,** the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

   [ ] the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

   b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

   [ ] contained in the international application in written form.

   [ ] filed together with the international application in computer readable form.

   [ ] furnished subsequently to this Authority in written form.

   [ ] furnished subsequently to this Authority in computer readble form.

   [ ] the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

   [ ] the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. [ ] **Certain claims were found unsearchable** (See Box I).

3. [ ] **Unity of Invention is lacking** (see Box II).

4. With regard to the **title,**

   [X] the text is approved as submitted by the applicant.

   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**

   [X] the text is approved as submitted by the applicant.

   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. 3

   [X] as suggested by the applicant.

   [ ] because the applicant failed to suggest a figure.

   [ ] because this figure better characterizes the invention.

   [ ] None of the figures.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/17395

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/16 G06K13/08 H05K5/02

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N G06K H05K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	EP 0 675 455 A (THOMSON CONSUMER ELECTRONICS) 4 October 1995 (1995-10-04) the whole document ---	4 1,7,10
Y	US 5 796 335 A (DROEGE HARTMUT ET AL) 18 August 1998 (1998-08-18) column 3, line 31 - line 43 ---	1,7,10
A	DE 31 10 670 A (STANDARD ELEKTRIK LORENZ AG) 30 September 1982 (1982-09-30) the whole document ---	4,7
A	EP 0 706 291 A (NEWS DATACOM LTD) 10 April 1996 (1996-04-10) the whole document --- -/--	3

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 October 2000	13/10/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Toussaint, F

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/17395

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 353 350 A (MAPSON MICHAEL ET AL) 4 October 1994 (1994-10-04) the whole document -----	1,7

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 00/17395

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0675455 A	04-10-1995	US 5455413 A	03-10-1995
		BR 9501218 A	30-01-1996
		CN 1125374 A	26-06-1996
		JP 7288797 A	31-10-1995
		SG 38833 A	17-04-1997
US 5796335 A	18-08-1998	DE 19600770 A	17-07-1997
DE 3110670 A	30-09-1982	DE 3020728 A	10-12-1981
		AT 378455 B	12-08-1985
		AT 227781 A	15-12-1984
		AU 7097881 A	10-12-1981
		CH 653831 A	15-01-1986
		FR 2483715 A	04-12-1981
		GB 2077013 A,B	09-12-1981
		SE 445962 B	28-07-1986
		SE 8102960 A	01-12-1981
EP 0706291 A	10-04-1996	IL 111151 A	24-09-1998
		AU 696725 B	17-09-1998
		AU 3303695 A	18-04-1996
		CA 2159779 A	04-04-1996
		JP 8214278 A	20-08-1996
		US 5666412 A	09-09-1997
		US 5774546 A	30-06-1998
		US 5878134 A	02-03-1999
US 5353350 A	04-10-1994	AU 645503 B	20-01-1994
		AU 6503490 A	28-04-1991
		WO 9105306 A	18-04-1991
		CA 2067331 A	04-04-1991
		EP 0494913 A	22-07-1992
		IL 95903 A	31-08-1995
		JP 5502956 T	20-05-1993
		ZA 9007902 A	31-07-1991

PATENT COOPERATION TREATY

EXPRESS EL902321798US

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

RECEIVED
AUG 14 2001
PCT IS&S

To:

SHONEMAN, David T.
THOMSON MULTIMEDIA LICENSING INC.
P.O. Box 5312
2 Independence Way
Princeton, New Jersey 08543
ETATS-UNIS D'AMERIQUE

DTS

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL PRELIMINARY EXAMINATION REPORT
(PCT Rule 71.1)

Date of mailing *(day/month/year)*	10.08.2001
Applicant's or agent's file reference RCA89673	**IMPORTANT NOTIFICATION**

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US00/17395	23/06/2000	15/07/1999

Applicant
THOMSON LICENSING S.A.

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.

2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.

3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

4. **REMINDER**

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Event	Notif. Final Countries IPER To Davida
Deadline	15 NOV 2001
Entered	DPF 8/16/01

Name and mailing address of the IPEA/	Authorized officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Schalinatus, D Tel.+49 89 2399-8242

Form PCT/IPEA/416 (July 1992)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
RCA89673		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US00/17395	23/06/2000	15/07/1999
International Patent Classification (IPC) or national classification and IPC H04N7/16		
Applicant THOMSON LICENSING S.A.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 14 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
09/02/2001	10.08.2001
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Loeser, E Telephone No. +49 89 2399 8482

Form PCT/IPEA/409 (cover sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/US00/17395

I. Basis of the report

1. With regard to the **elements** of the international application *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17))*:
Description, pages:

1-9	as received on	27/12/2000	with letter of	27/12/2000

Claims, No.:

1-10	as received on	27/06/2001	with letter of	25/06/2001

Drawings, sheets:

1,2	as received on	27/12/2000	with letter of	27/12/2000

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   - ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
   - ☐ the language of publication of the international application (under Rule 48.3(b)).
   - ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   - ☐ contained in the international application in written form.
   - ☐ filed together with the international application in computer readable form.
   - ☐ furnished subsequently to this Authority in written form.
   - ☐ furnished subsequently to this Authority in computer readable form.
   - ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   - ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

   - ☐ the description, pages:
   - ☐ the claims, Nos.:

☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-10
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-10
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1-10
	No:	Claims	

2. Citations and explanations
see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:
see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:
see separate sheet

1. General

The present application does not satisfy the criteria set forth in Article 6 PCT. Details of the objections are set out below. The invention is industrially applicable.

2. Concerning Section VIII - Art. 6 PCT:

2.1. Claim 1

2.1.1.

According to the description, the invention has to objectives:

(a) preventing hacking;

(b) EMI/RFI shielding of an apparatus having an aperture.

The claimed feature "a conductor formed along a path substantially encompassing an area between spaced edges ..." is obscure (Art. 6 PCT contravened). It is considered that the passage underlined above should read "encompassing a substantial area" for clarification and in order to provide a feature that is essential to meet each of the two objectives identified above (e.g., if the area covered by the conductor is less than a substantial portion of the cover, then breaching of the cover by e.g. drilling a hole cannot be detected).

2.1.2.

The claim's features "supplying an electrical signal to the conductor formed in the port cover" and "monitoring the electrical signal ..." respectively fail to specify the origin of the electrical signal and the location where the monitoring is effected. According to these features, both the signal supply and the monitoring could be effected by an operator using means that are neither part of the port cover nor of the host device.

The broad scope of these features lacks support by the description (Art. 6 PCT contravened) which appears to merely disclose that the signal is supplied by the host device, and that the monitoring is effected in the host device.

2.2. Claim 4

2.2.1

The claimed feature "operable for at least one of providing an electromagnetic shield ... and providing one or more conductors that are continuous absent an opening being formed in the port cover to break one of the conductors" is obscure as such (in particular, the word "absent" does not appear to be appropriate, a construction using e.g. "except if an opening is formed" is suggested instead).

Moreover, by the statement "at least one of" in the passage identified above the claim provide all the features that are essential to meet the objectives of the invention (cf paragraph 2.1 above; Art. 6 PCT contravened).

2.2.2

With the claimed feature "wherein the port cover is coupled to the host device in such a way that ..." an attempt is made to define the subject-matter in terms of the result to be achieved which merely amounts to a statement of the underlying problem (Art. 6 PCT contravened). The technical features (means) necessary for achieving this result should be added.

2.2.3

As set out in relation to claim 1 (see section 2.1.2 above), it is considered that the claim fails to out clearly the means by which intrusion protection is carried out. Overcoming this objection would require specifying means for supplying a signal to the conductor in the port cover and means arranged in the host device for monitoring that signal.

3. Concerning Section V - Articles 33(2) and 33(3) PCT

The following documents are cited - the numbering will be adhered to in the rest of the procedure:

D1: EP-A-0 675 455;

D2: US-A-5 796 335;

D3: US-A-5 353 350.

3.1. Claim 1

3.1.1.

D1 at least implicitly discloses a method of securing information being transferred, as defined in the header portion of claim 1. D1 further discloses the positioning of a port cover 13 over the disclosed port (Fig.1 Ref. 11).

D2 discloses the use of a security foil for shielding (abstract) and simultaneously for intrusion protection (Fig.3; col.3 lines 16-45). For these purposes, a meandering conductor (security foil) is formed across a surface or device. According to D2, the meandering conductor can be used to envelop a security module (such as a smart card or an information storing device as defined in claim 1) that can be inserted in an "overall unit" (col.3 lines 16-24).

When the thus protected security device is inserted in the overall unit, the device's shielding is connected to a frame terminal of the unit (col.3 lines 16-22).

D2 further discloses monitoring by a security circuit (col.2 line 47) connected to the meandering conductor so as to detect shorting of impairing thereof by mechanical impact.

D3 discloses another solution to present intrusion in a device.

None of the available documents discloses a port cover having a conductor formed therein as claimed in claim 1.

3.1.2.

Using a cover to protect an aperture of a housing from mechanical damage and dust is also well-known in the art, so that such a concept cannot establish an inventive step.

Problems of electromagnetic interference are well-known in the art. Thus shielding of an apparatus or shielding an aperture of a housing by using an appropriately designed cover cannot establish an inventive step either.

According to D2 shielding and simultaneous intrusion protection is established only for the security device. It does not

enable such effects for a combination of host and information storing device when the latter is arranged in the host's port.

One cannot fairly conclude that the skilled person attempting to improve the port cover disclosed in D1 would have arrived at the features of claim 1 without exercise of inventive step.

It is thus considered that notwithstanding the objections under Art. 6 PCT raised in paragraph 2.1 above both novelty and inventive step can be associated with claim 1.

3.2. Claim 4

The findings set out in paragraph 3.1 above with respect to claim 1 correspondingly apply to claim 4, despite the latter's remaining deficiencies concerning clarity set out in paragraph 2.2 above.

4. Concerning Section VII: Description and other belongings

4.1. The claims are not cast in the two-part form as required by Rule 6.3(b) PCT.

4.2. Documents reflecting the prior art described on pages 1-2 are not identified in the description (Rule 5.1(a)(ii) PCT).

4.3. Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in the documents D1-D3 cited above is not mentioned in the description, nor are these documents identified therein.

4.4. The description is not in conformity with the claims as required by Rule 5.1(a.iii) PCT. This objection can by overcome by making references to at least the independent claims.

PORT COVER FOR LIMITING TRANSFER OF ELECTROMAGNETIC RADIATION FROM A PORT DEFINED IN A HOST DEVICE

BACKGROUND OF THE DISCLOSURE

1. Field of the Invention

The invention relates to host devices. More particularly, the invention relates to a port cover for a host device.

2. Description of the Prior Art

Smart cards, and other similar information-storing devices, are known for their capabilities in storing information relating to stored funds, personal identification and other personal data, descrambling keys and an ability to access certain host devices.When multiple users share a common host device, each user may have a separate smart card having selected limitations, these limitations are triggered, e.g., when one user's smart card is removed from a host device and another user's smart card is inserted into the host device.

It is difficult to provide an interface between smart cards and certain host devices that emit certain ranges of electromagnetic radiation. For example, satellite receivers formed as set top boxes are configured as enclosed boxes with an electromagnetic/radio frequency interference shield (EMI/RFI shield) entirely covering each wall of the satellite receiver. If a satellite receiver is provided with a smart card port to provide access to the smart card, the smart card port would provide an opening in which little or no EMI/RFI shield would exist. With a lack of an EMI shield over even a portion of the host device, electromagnetic interference (EMI), possibly including radio frequency interference (RFI), could escape from the satellite receiver into the surrounding space. This large emission of EMI is unacceptable, since it does not conform with industry standards and can result in interference applied to electronic equipment located in the vicinity.

It would be desirable to provide a configuration for a host device having a smart card port in which the entire satellite receiver can be shielded to limit emissions of EMI generated by the host device into the surrounding areas.

Hackers present another concern by attempting to "use" information obtained from other smart cards. One technique that accomplishes this unauthorized accessing of information is referred to as hot-wiring a smart card. This hot-wiring is accomplished by affixing a single wire to each smart card contact. The smart card is then inserted into the host device and the host device begins to interact with the smart card with the hot-wiring wire extending out of the port. During this interaction, confidential information may be electronically

transferred between the host device and the smart card, and thereby is also transmitted outside of the host device through the hot-wiring wires, via the port. If a hacker uses suitable equipment outside the host device, the hacker can obtain much of the confidential information that is on the smart card, and can also produce a copy of the smart card that might be used in place of the original.

Therefore, a need exists in the art for a device to limits hot-wiring of the smart card. This device will improve security associated therewith by preventing unauthorized use of access codes and breach of confidentiality, thereby improving user confidence in, and acceptance of, the system.

SUMMARY OF THE INVENTION

The present invention relates to a port cover for covering the port formed in a host device, the port cover includes a bottom portion, a plurality of side portions, and couplers to attach the sides to a host device, where said couplers attach on either side of the port.

BRIEF DESCRIPTION OF THE DRAWINGS

The teachings of the present invention can be readily understood by considering the following detailed description in conjunction with the accompanying drawings, in which:

FIG. 1 shows a schematic diagram of a satellite/TV receiver system in accordance with one embodiment of the present invention;

FIG. 2 shows a cross sectional expanded view of a smart card inserted into a host device in accordance with one embodiment of the present invention;

FIG. 3 shows a partial cross-sectional view of one embodiment of a port cover in accordance with the present invention;

FIG. 4 shows a perspective view of one embodiment of the port cover of FIG. 3;

FIG. 5 shows a perspective view of an alternate embodiment of the port cover 302 of Fig. 3.

To facilitate understanding, identical reference numerals have been used, where possible, to designate identical elements that are common to the figures.

DETAILED DESCRIPTION

After considering the following description, those skilled in the art will clearly realize that the teachings of the invention can be readily utilized in satellite/TV receiver systems, or any other host device that uses a smart card or other similar information-storing device.

FIG. 1 shows a typical satellite/TV receiver system 100 that includes a satellite receiver 101, a satellite dish 102, and a television 104. The integration and operation of system 100 (particularly controller 107, CPU 114, memory 116, I/O 118 and bus 119) is well known and thus is not described herein

Satellite receiver 101 includes smart card portion 106 and controller portion 107. Smart card portion 106 includes the removable smart card 108, a smart card port 112, a smart card collar 113, and a smart card reader 110. The smart card reader 110 includes smart card reader head 111. In one embodiment, the smart card 108 includes a smart card operating patch 109. The smart card port 112 permits insertion of, and removal of, different selected smart cards through the smart card port 112. Smart card collar 113 retains the smart card 108 in position when a smart card 108 is inserted through the smart card port 112. The smart card port 112 is formed in a housing 121 that defines the outer surface of the satellite receiver 101.

Smart card 108 is further detailed in cross section in FIG. 2. Smart card operating patch 109, formed on an external surface of smart card 108, includes smart card contacts 202a, 202b, 202c, and 202d, integrated circuit 205, and insulative material 204 (e.g., resin) that secures contacts 202 in position. Each smart card contact is electrically connected by conductors to integrated circuit 205. The surface of each smart card contact is exposed to an external surface 201 of smart card 108 at smart card operating patch 109 such that an electric probe touching the exposed surface at each smart card contact can transmit signals to, and receive signals from, the integrated circuit 205. The primary function of integrated circuit 205 (which may be an application specific integrated circuit) is to store information (some of which may be modified). The information that is to be saved may include monetary amounts, programming capabilities, individual and address information, and other such information, such as descrambling keys.

The smart card reader 110 is also depicted in FIG. 2 in a position that it would be when interacting with the smart card contacts. The smart card reader 110 includes a plurality of smart card contacts 206a, 206b, 206c, and 206d which electrically connect to smart card contacts 202a, 202b, 202c, and 202d, respectively, when the smart card is inserted in the smart card port 112. Although four smart card contacts 206a-d are depicted in FIG. 2, any suitable number of smart card contacts can be selected for the intended task, such as, e.g., eight depicted in FIG. 3.

During use, different smart cards may be removed from, and inserted into, satellite receiver 101. In a household, for example, different members may have different television channels that their smart cards can access, or certain users may by allowed only a certain amount of use of the satellite receiver 101 (and the associated television 104) each week. Any card, chip, or other device that provides similar interactive capabilities with a host device as described herein is intended to be within the scope of the smart card of the present invention. Any host device capable of interacting with a smart card, such as a television set-top cable or satellite box, flash memory modules used in digital cameras, so-called MP players, etc. are within the intended scope of the present invention.

Two problems exist relative to the above-mentioned smart card 108 and host device 101 configuration that a port cover 302, shown in FIG. 3 and described below, is intended to overcome. A first electromagnetic interference (EMI)/ radio frequency interference (RFI) shielding problem results from the EMI or RFI produced by the satellite receiver 101. Typically, the housing 121 of satellite receivers 101 are formed to shield electromagnetic radiation. The smart card port 112 however defines a breach in the EMI/RFI shielding by which the EMI/RFI can escape form the host device or satellite receiver 101. Such a breach in the EMI/RFI shielding in the satellite receiver severely limits the approval of the satellite receiver 101 by appropriate governmental communication radiation regulatory agencies.

A second, security related, problem with smart cards results when any unauthorized smart card user attempts to access either the host device or information contained in the smart card. The fact that the smart card operating patch 109 is physically located within the satellite receiver 101 as shown in FIG. 1 is a first effort to limit unauthorized users from gaining access to the information contained within the smart card, when the smart card 108 is positioned within the satellite receiver 101 by limiting unauthorized users access to the smart card contacts 206a-d. One technique by which unauthorized users gain access to information contained within the smart card 108 is to electrically connect a distinct, appropriately sized, electrically conductive wire (referred to herein as hot-wired wire 212 depicted in FIG. 2) to each distinct smart card contact 202a, 202b, 202c, and 202d. Thus, when the smart card 108 is inserted into the smart card port causing each smart card contact 202 to contact the respective reader head contact 206, then any signal transmitted between the smart card reader head 111 and the smart card 108 could be read at the other end of the hot-wired wire 212, which would extend out of the smart card port

112. This unauthorized accessing of information contained in the smart card is referred to herein as "hot-wiring" the smart card.

Port Cover

Port cover 302 is mounted over smart card port 112 after the smart card is inserted into the smart card port. The use of the port cover 302 has two primary functions. First, the port cover 302 limits EMI (including RFI) that can escape from the EMI/RFI shield after the port cover is in place. Second, the port cover 302 limits the use of the host device (e.g. satellite receiver 101) if the smart card 108 is being hot-wired. With the port cover 302 in place, the remote end of the hot-wired wires 212 cannot physically extend from within the satellite receiver 101, through the smart card port cover 302, to outside of the satellite receiver. The port cover 302 is preferably configured as a snap-on, electroless metal plated plastic cover. The port cover 302 is configured to cover the port while a National Renewable Security Standard (NRSS) smart card 108, or the like, is installed therein.

Port cover 302 includes body portion 303, peripheral mounting surface 304 coupling pads 306a and 306b, mounting flanges 308, and small spherical bumps 416. Body portion 303 forms the cover to limit access into the smart card port 112. Body portion 303, depicted in FIG. 3, includes bottom portion 330, and multiple side portions 330, 334, 336 that extend from the peripheral mounting surface 304 to the bottom portion 330. The bottom portion 330, side portions 330, 334, and 336, and peripheral mounting surface (when the port cover 302 is installed) define an enclosure that combines with the satellite receiver 101 to delineate an interior space where the satellite receiver 101 components are located from an outside space 322. Radiation contained within the interior space is shielded from passing into the outside space 322. A peripherally extending surface 309 is formed in the housing 121 and extends around the periphery of the smart card port 112. A peripheral mounting surface 304 mounts with the peripherally extending surface 309 in a manner that no wires can extend between the two surfaces when the port cover 302 is installed.

Coupling pads 306a, 306b have two functions. First, each distinct coupling pads 306a, 306b enter into a distinct mating recesses 310 to securely position the port cover 302 over smart card port 112. Second, coupling pad 306a contacts electrical source contact (not depicted but contained in first mating recess 310 that coupling pad 306a engages with) while coupling pad 306b contacts electrical drain contact (not depicted but contained in second mating recess 310 that coupling pad 306b engages with) causing an electrical

voltage to be applied as described below. Mounting flanges 308 also extend into recesses 314 to assist in securing the port cover 302 to the peripherally extending surfaces 309. Port cover 302 is preferably formed form a resilient plastic that permits the coupling pads 306a, 306b, and the mounting flanges 308 to be displaced relative to each other as a result of a moderate biasing force. This relative displacement permits the coupling pads to be inserted into the mating recesses 310, and the mounting flanges 308 to be inserted into the recesses 314 to a position where tangs 340 snap back into position and secure the port cover in position covering the entire port cover. When the tangs 340 are securing the port cover in position, release portions 342 may be pressed to deflect the tangs, and release the coupling pads 308 from the mating recesses 310 while the mounting flanges 308 are removed from recesses 314. Small spherical bumps 416 extend from the peripheral mounting surface 304 to ensure grounding of the peripheral mounting surfaces 304 to the peripherally extending surface 309, thereby grounding port cover 302 to housing 121.

Formed in housing 121 of satellite receiver 101 is EMI/RFI shield 320. However, the EMI/RFI shield 320 does not extend over smart card port 112 which defines a breach in the EMI/RFI shield. To limit escape of EMI/RFI that passes through smart card port 112 into the surrounding environment (depicted as 322 in FIG. 3), port cover 302 is provided with EMI/RFI cover shielding 322, which is selected to be a suitable material to shield the EMI or RFI that is likely to be produced within the satellite receiver 101. As the port cover is positioned such that: a) coupling pads 306a, 306b are positioned within mating recesses 310, b) mounting flanges 308 are positioned into recesses 314, and c) peripheral mounting surface 304 abuts peripherally extending surface 309; then EMI/RFI enclosure 324 is formed within EMI/RFI cover shield 322 that limits passage of EMI and/or RFI from within the EMI/RFI cover shield to the surrounding environment 322.

The use of hot-wired wires by hackers to tamper with or access information contained on smart card 108 has been described above. There are two embodiments of port covers 302 depicted in FIGs. 3, 4, and 5 that limit the use of hot-wired wires 212. In considering the two embodiments of port covers 302, FIG. 3 should be viewed in combination with FIG. 4 for the first embodiment. FIG. 3 should be viewed in combination with FIG. 5 when considering the second embodiment.

There are two distinct embodiments of the present invention depicted in FIGs. 4 and 5, respectively. Both embodiments of the present invention limits access of information across the hot-wired wire to a remote end of the hot-wired

wire from the contact 202a, via the smart card port 112 to a location outside the port cover 302. Since the entire length of the hot-wired wire 112 would be either positioned within either the host device; e.g., the satellite receiver 101, or the port cover 302, a hacker is restricted from accessing a hot-wired wire 212 when the port cover 302 is in place.

The first embodiment of the present invention (depicted in FIG. 4) involves the use of a conductor trace 412. Conductor trace 412 functions to limit an unauthorized user from drilling through the port cover 302 such that hot-wired wires 212 can be passed through the holes in port cover 302. The conductor trace covers top portion 330, front portion 332, bottom portion 334, and the two side portions 336. The conductor trace 412 is to be configured such that if a hacker drills through the port cover 302 at any location that might provide access for the hot-wired wires 212, then at least one individual conductor 414 in conductor trace 412 will be severed. The individual conductors 414 of the conductor trace 412 are preferably arranged in parallel. Therefore, severing of any of the individual conductor(s) 414 will alter the electrical characteristics (e.g., the impedance) of the entire conductor trace 412. Therefore, the conductor trace can be monitored for changes in impedance, indicating tampering of port cover 302. Additionally, if port cover 302 is not positioned over smart card port 112, then the coupling pads 306a and 306b will not engage with mating recess 310 and electric current will not pass between the two mating recesses 310 associated with two coupling pads 306a and 306b.

It is preferable for the conductors to form conductor trace 412 to cover as much of the surface area of port cover 302 as possible, with as little spacing between the individual conductors 414 of the conductor trace as possible. This will limit the possibility that a hacker will be able to drill between the individual conductors 414 forming the conductor trace 412 in that the hacker may attempt to cut or drill around the individual conductors, if they can see where they are located.

There are a variety of techniques by which conductor trace 412 is formed. In a first conductor trace formation technique, the conductors are applied to the port cover via selective plating or conductive powder coating. In selective plating, a conductive material is plated onto the surface of the port cover 302. A conductive material that can adhere to the material that the port cover is formed from (preferably plastic), is required. In conductive powder coating, an adhesive (not shown) following the outline of the individual conductors is placed on the desired surfaces of the port cover 302, and a powder formed from a conductive material is applied to the adhesive. The conductive powder "sticks" to the

adhesive, thereby forming the conductors in the conductor trace 412. In an alternate embodiment, the individual conductors 414 of the conductor trace 412 are affixed to the port cover 302 by a resin such as epoxy. The surface above the individual conductors of the conductor trace 412 should be painted so hackers cannot determine the precise positioning of the individual conductors 414 in the conductor trace 412. The technologies used to form the conductor trace are generally known, and will not be further detailed herein. Any known technique by which a conductor trace 412 is applied to port cover 302 is within the scope of the present invention.

Even though the term "electric current" is used in this specification and the associated claims, it is intended that related electrical measurements such as electric voltage, electrical voltage or current of a prescribed frequency or waveform, etc., are within the scope of the present invention. It is also envisioned that magnetic characteristics can be measured across the conductor trace 412 using known detector systems that can interface with controller 107. The conductor trace 412 may be configured as either an active or passive circuit. However, any technique that securely attaches, or forms, the individual conductors 414 to the port cover 302 is within the intended scope of the present invention.

In the second embodiment of applying conductor trace 412 to port cover 302 (depicted in FIG. 5 as taken relative to FIG. 3), the conductor trace 412 in the FIG. 4 embodiment is replaced by conductive plating 500 (shown by shading) applied to the port cover 302. More specifically, the conductive plating extends over top portion 330, front portion 332, bottom portion 334, and the two side portions 336. The conductive plating 500 is connected by insulated conductors 504a, 504b to coupling pads 306a, 306b, respectively. Alternatively, the above-described conductive plating and conductive powder technologies, described relative to the FIG. 4 embodiment, may be applied in this embodiment as well to form a substantially continuous conductor over the port cover 302. Insulated conductors 504a and 504b are depicted as attached to the surface of peripheral mounting surface 304 in FIG. 5, however the insulated conductors may actually be integrated in port cover 302. Conductive plating has empirically determinable electrical resistivity characteristics that are altered by tampering, such as cutting through, or drilling in, the body portion 303. Inner or outer surfaces of conductive plating 500 may contain an insulative coating (not shown) to limit grounding of the conductive plating 500 to the port cover 302. This insulative coating is not necessary if the port cover 302 is formed from an insulative plastic. As a result of such cutting or drilling in the body portion 303,

which will necessarily cause similar cutting or drilling of the conductive plating 500 that plates the body portion 303, the electrical characteristics of the conductive plating 500 will be altered. This altering of the electrical characteristics of the conductive plating 500 can be sensed as a varying impedance, resistance, or other measurement in a similar manner that the electrical characteristics of the electrical trace 412 was altered in the FIG. 4 embodiment when individual conductors were severed.

The FIGs. 3 and 4 port cover embodiment, as well as the FIGs. 3 and 5 port cover embodiment, may be controlled by controller 107 as depicted in FIG. 1. Considering the above disclosure, controller 107 may encounter three possible alternative conditions relating to the electric level of the electric contacts formed in mating recess 310 (not shown):

a) when no electric current is sensed between the electric contacts formed in the two mating recesses 310, controller 107 determines that there is no port cover 302 in place. Under these conditions, controller 107 will not interact with the smart card 108;

b) when a predetermined limit of electric current is sensed between the electric contacts formed in the two mating recesses 310, controller 107 determines that the port cover is in place, and none of the individual conductors 414 in the conductor trace 412 have been tampered with. Under these circumstances, controller 107 will interact with the smart card 108; or

c) when some range of electric current between the "no electric current" sensed in part a) and the "predetermined limit" of part b) is sensed between the electric contacts formed in the two mating recesses 310, controller 107 determines that at least one of the individual conductors 414 in the conductor trace 412 have been tampered with (e.g., a conductor has been damaged, presumably by drilling or cutting through the port cover 302). Under these circumstances, controller 107 will not interact with the smart card 108.

The level of the predetermined limit is based on the specific circuit, and is preferably determined empirically.

Though various embodiments which incorporate the teachings of the present invention have been shown and described in detail herein, those skilled in the art can readily devise many other varied embodiments that still incorporate these teachings.

CLAIMS

1. A method of securing information being transferred from an information-storing device (108) interacting with a host device (106) through a port (112) formed in the host device (106), the port (112) being configured to receive the information-storing device (108), the method comprises the acts of:

providing a port cover (302) having a conductor (412, 414, 500) formed therein along a path substantially encompassing an area between spaced edges (330, 334, 336) of the port cover (302);

positioning the port cover (302) over the port (112) and coupling it to the host device so as to block the port (112);

supplying an electric signal to the conductor (412, 414, 500) formed in the port cover (302); and

monitoring the electric signal to ensure that the port cover (302) is correctly positioned and not breached.

2. The method set forth in claim 1, further comprising the act of limiting interaction by a host device (106) with the information-storing device (108) if the monitored electric signal exceeds a predetermined parameter.

3. The method set forth in claim 1, wherein the host device (106) is a satellite receiver (101).

4. An apparatus for use with a smart card, the apparatus comprising:

a host device (106) capable of accessing information stored in the smart card (108), the host device (106) including a housing (121) having a port (112) formed therein, the port (112) is configured to receive the smart card (108), when the smart card (108) is inserted into the port (112), information can be transferred from the smart card (108) to the host device (106);

a port cover (302) removably coupled to the housing (121) surrounding the port (112), wherein the port cover (302) physically blocks the port;

wherein the port cover (302) comprises at least one conductor (412, 414, 500) that is coupled to the host device and is operable for at least one of providing an electromagnetic shield across the port (112) and providing one or more conductors (414) that are continuous absent an opening being formed in the port cover (302) to break one of the conductors (414), and wherein the port cover (302) is coupled to the host device (106) in such a way that the host device (106) detects discontinuity of the port cover (302).

5. The apparatus set forth in claim 4, wherein a data stream can be transferred between the smart card (108) and the host device (106), when the smart card (108) is inserted in the port and the port cover (302) is covering the port.

6. The apparatus set forth in claim 4, wherein when the port cover (302) is installed, electrical wires (212) electrically connected to the smart card (108) are limited from extending through the port (112) from within the host device (106) to outside of both the host device (106) and the port cover (302).

7. The apparatus set forth in claim 4, wherein the housing (121) includes a mounting flange (308) extending peripherally of the port (112), wherein when the port cover (302) is attached to the mounted flange (308), the port cover (302) covers the entire port (112) such that the housing (121) and the port cover (302) define an enclosure.

8 The apparatus set forth in claim 4, wherein

at least one conductor (414) is attached to the port cover (302);

an electric sensor (107) sensing a breach of the conductor; and

a limiting device (114) limiting operation of the host device (106) when the conductor (414) is breached.

9. The apparatus set forth in claim 4, wherein the conductor comprises a plurality of wires (414) arranged in parallel extending across the port cover (302).

10. The apparatus set forth in claim 4, wherein the conductor comprises a conductive plate (500).

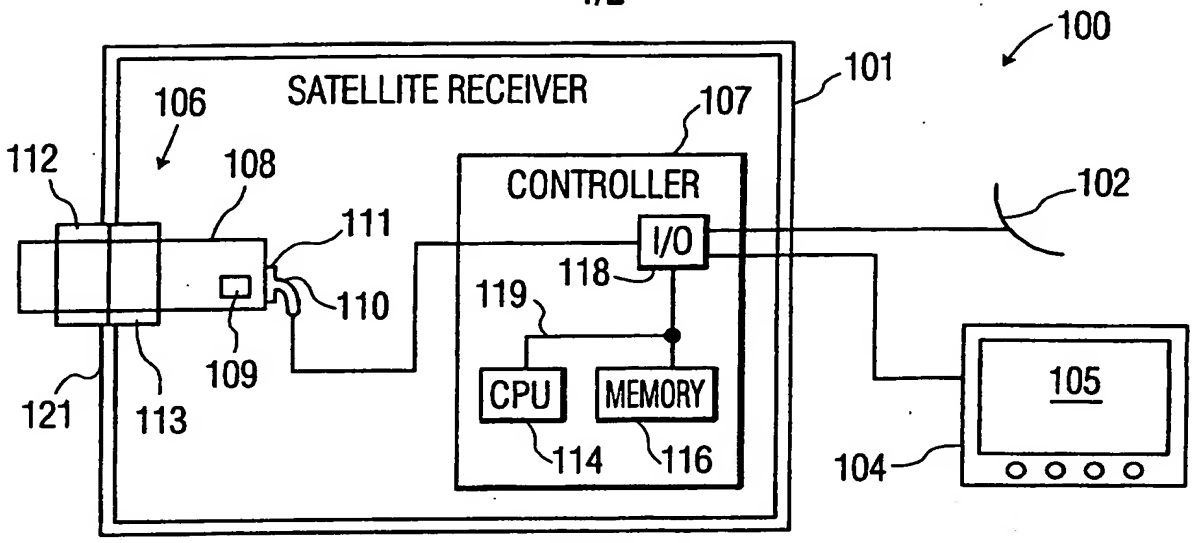

FIG. 1

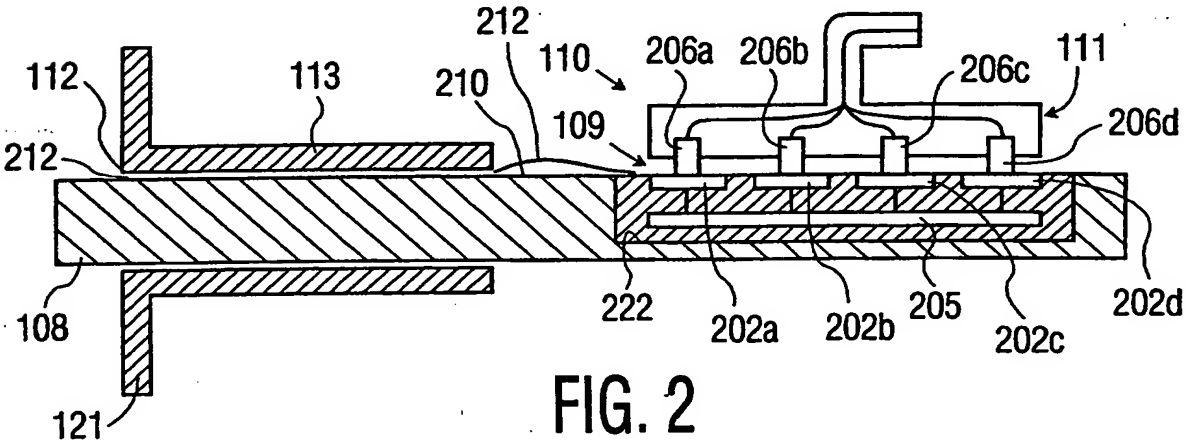

FIG. 2

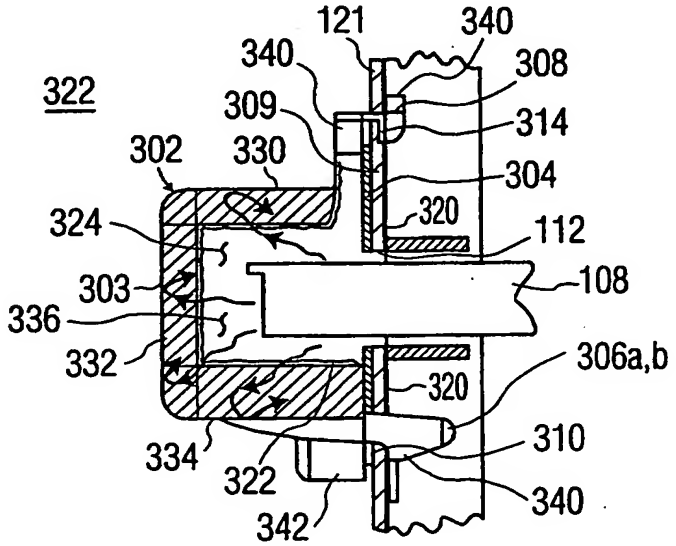

FIG. 3

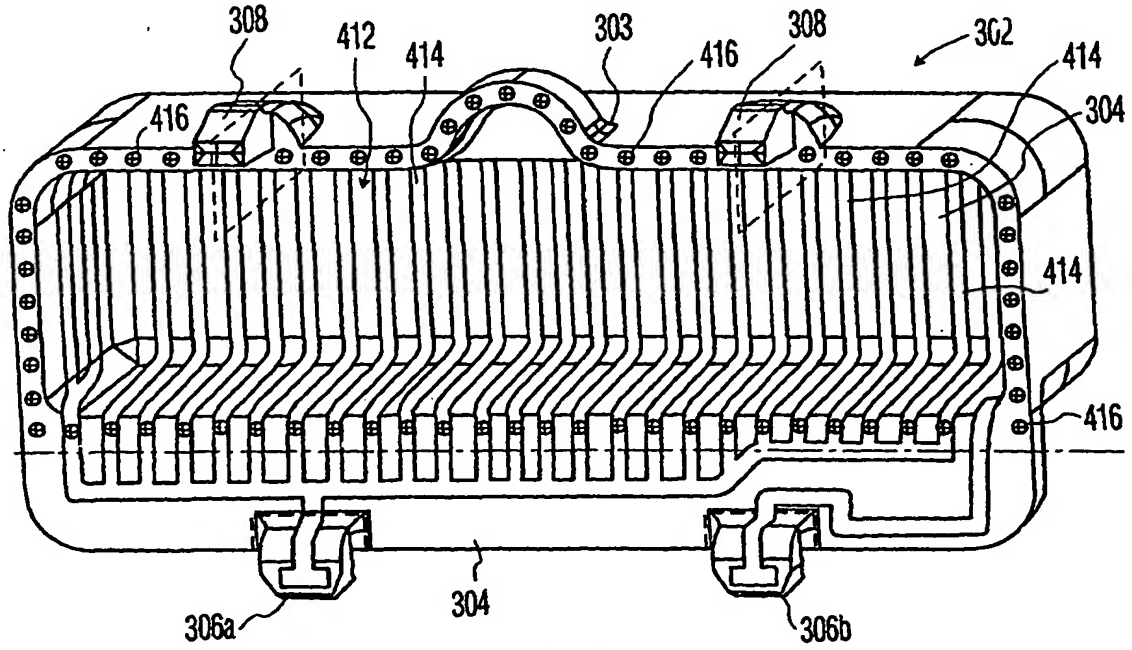
308
412
414
303
416
308
302
414
304
416
414
416
306a
304
306b

FIG. 4

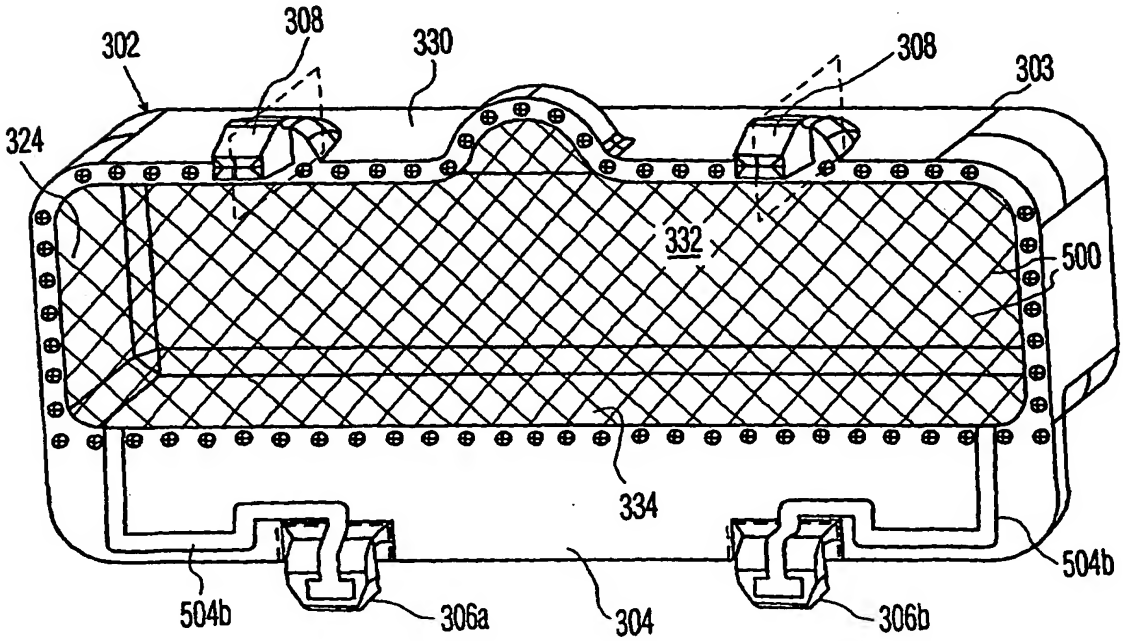
302
308
330
308
303
324
332
500
334
504b
504b
306a
304
306b

FIG. 5